

## UNITED STATES DISTRICT COURT

for the  
District of AlaskaIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Information associated with an Apple iCloud account with  
DS ID 1972828024 that is stored at premises controlled  
by Apple, Inc.

Case No. 3:16-mj-00204 DMS

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated here by reference.

located in the \_\_\_\_\_ District of \_\_\_\_\_ Alaska \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated here by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 USC § 1030

Computer Fraud

Offense Description

The application is based on these facts:

See attached Affidavit in Support of Search Warrant.

☒ Continued on the attached sheet.☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth in the attached \_\_\_\_\_ sheet.

Signature Redacted

\_\_\_\_\_  
applicant's signature

Elliott Peterson, Special Agent, FBI

\_\_\_\_\_  
Printed name and title

Sworn to before me and signed in my presence.

Date:

5/20/16

/s/ DEBORAH M. SMITH  
CHIEF U.S. MAGISTRATE JUDGE  
SIGNATURE REDACTED\_\_\_\_\_  
Judge's signature

City and state: Anchorage, Alaska

DEBORAH M. SMITH, U.S. MAGISTRATE JUDGE

\_\_\_\_\_  
Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH AN  
APPLE ICLOUD ACCOUNT WITH DS ID  
NUMBER 1972828024 THAT IS STORED  
AT PREMISES CONTROLLED BY APPLE

Case No. 3:16-mj-00204 DMS

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Elliott Peterson, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with the above-listed Apple ID that is stored at premises controlled by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications and stored data) further described in Attachment A. Upon receipt of the information described in Attachment A, government-authorized persons will review that information to locate the items described in Attachment B.

2. I am employed as a Special Agent (S/A) for the Federal Bureau of Investigation (FBI). I have been so assigned for over four years. I am assigned to the FBI Anchorage Field Office, Anchorage, Alaska. My duties and responsibilities include investigation of complex computer crimes to include malware based account takeover fraud, large scale botnets, and Distributed Denial of Service (DDOS) attacks. I have experience investigating botnets which



utilize various forms of encryption and communication protocols, to include those utilizing Peer to Peer (P2P) communication protocols.

3. I have graduated from the FBI Academy in Quantico, Virginia, and attended other training offered by the FBI and other groups on computer and network technology. I have a bachelor's degree in Computer Science.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. The facts set forth in this affidavit are based on my personal knowledge, the knowledge obtained during my participation in this investigation, the knowledge obtained from other individuals, including other law enforcement personnel, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, this affidavit does not set forth each and every fact learned by me during the course of this investigation.

6. The items to be searched for and seized consist of evidence and instrumentalities of violations of Title 18, United States Code, Section 1030 (Computer Fraud).

**RELEVANT FEDERAL LAW**

7. Under 18 U.S.C. § 1030(Computer Fraud), it is unlawful for anyone to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer, and cause damage affecting 10 or more protected computers during any one-year period. 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B).



**JURISDICTION**

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

**INVESTIGATION**

9. Kelihos is a name utilized by internet security experts to describe a computer virus (also known as malware) that has been actively engaged in spam distribution schemes since at least 2012. Like many computer viruses, Kelihos has been extensively studied since its detection. Your Affiant has studied Kelihos through several methods: reviewing published papers on the malware, interviewing internet security experts who specialize in Kelihos and Peer to Peer botnets, and my own analysis of the actual malware.

10. “Internet Protocol address” or “IP address” is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISP) assign IP addresses to their customers' computers. ISPs typically log their customers' connections, which means that the ISP can identify which of their customers was assigned a specific IP address during a particular session.

11. “Server” is a centralized computer that provides services for other computers connected to it through a network. The computers that use the server's services are sometimes




called "clients". Server computers can be physically located anywhere. For example, it is not uncommon for a network's server to be located hundreds, or even thousands of miles away from the client computers.

12. "Malware", short for malicious software, is software used or programmed by hackers to disrupt computer operations, gather sensitive information, or gain access to otherwise private computer systems.

13. "Emails" sent over the Internet contain IP addresses that can be used to determine the origin and destination of the message. The "header" of an email, which is attached to the top of every email and contains IP addresses of computers which have transmitted the email, may be used to identify the "path" through the internet the email traveled from its origin to its destination. The header will often contain the IP addresses of any and all servers from which the given email "bounced" en route to its destination. These IP addresses may be traced to determine the sender of a specific email.

#### Botnets

14. Kelihos is a class of computer virus known as a "botnet", indicating that the virus results in a number of computer infections centrally controlled by parties other than the legitimate owner of the computer. By definition, this control is without the authorization of the legitimate owner. There are many different types of botnets, but they are generally organized by their purpose, which can include Account Takeover Fraud, Spam Distribution, Bitcoin Mining, and Data Exfiltration. Botnets are also described according to their Command and Control (C2) communication protocols. A C2 communication protocol is the method that a botnet operator uses to communicate with the infected computers. Kelihos is a botnet used primarily for spam email distribution and utilizes a Peer to Peer, or P2P communication protocol.



15. Your Affiant has previously investigated both spam email distribution botnets and botnets utilizing P2P communication protocols. Based upon my training and experience, your Affiant knows that some of the most common uses of spam email distribution botnets are distributing other computer viruses, promoting affiliate programs such as pornography website subscription generation schemes, and facilitating the online sale of grey-market pharmaceuticals and stock market “pump and dump” schemes.

16. Similarly, your Affiant is aware that botnets utilizing a P2P communication protocol rely upon the compromised victims themselves to serve as proxies for virus communication. This is intended to obfuscate the administration of the botnet by its operators, make the botnet more resilient to takeover operations, and to make investigation more challenging for law enforcement agencies. A traditional C2 architecture results in every infected computer communicating directly with the C2 server. This is generally a two way exchange of data, with the server issuing requests or commands, and the victim responding. It is more common now to see botnets using proxies to comprise the majority of a C2 network. Proxies are servers configured as relays, so that all data received from Victim A is sent to Proxy B, which then transmits the data to Server C. This works in reverse, with commands from Server C sent to Proxy B which are transmitted to Victim A. Utilizing a proxy in this manner conceals the true location of a C2 server, and generally, botnet operators place both proxies and C2 servers in locations or formats inaccessible to law enforcement.

#### Internet Forums

17. Kelihos is believed to be a variant or improvement of the Storm Botnet. This is because the two viruses share commonality in function, suspected source of origin, and administration. Storm and Kelihos have both been advertised for sale on online criminal forums



by an individual who identified himself as “Peter Severa” or “Severa”. Examples of well known criminal forums on which the nickname Severa has been utilized include darkode.com, verified.cm, spamdot.us, antichat.ru, directconnection.ws, and carderplanet.com. On the forum carderplanet.com, “Severa” utilizes a signature block which includes the label “Professional Bulk Mailings.”

18. It is common for criminals engaged in computer crime to utilize nicknames, especially on the criminal forums on which they exchange data on criminal techniques and offer products and services for sale. The use of nicknames allows them to protect their true identity, while still allowing for the benefits of name and product recognition. While there are a large number of Internet forums devoted to the exchange of criminal services and techniques, many criminals will use the same nickname on different forums. This is likely due to perceptions of anonymity, as well as the reliance upon reputations tied to nicknames. In these communities, actors are known principally by either their given nickname, or an email, jabber, or ICQ handle. These reputations become very important both in the exchange of data, and access to marketplaces in which products and services are sold. Upon examination of many criminal forum accounts in the name “Severa,” your Affiant has noted that in the majority, the ICQ number 104967 is utilized. ICQ is a popular Internet instant message service in which users are identified by unique numerical values, known as ICQ numbers. Based upon my training and experience your Affiant knows that ICQ numbers are rarely changed or transferred by online criminals. Therefore your Affiant concludes that the combination of identical ICQ number and nickname are indicative of the same individual accessing and utilizing these accounts. Other commonalities include the overlapping use of email accounts and jabber accounts.



MAY 20 2016



19. Jabber is an Internet instant messaging protocol. Instead of utilizing numeric values, Jabber handles function similarly to email addresses, with the first value being a unique user identifier, and the second value being the domain name that is responsive to the Jabber communication protocol. Jabber has become one of the preferred communication methods utilized by online criminals because it can support full Off the Record Messaging, a fully encrypted method of exchanging instant messages. Also, Jabber is a protocol, as opposed to a service, so responsive user records are maintained on individual servers. Many criminals choose to run their own Jabber servers, making them inaccessible to law enforcement through service providers.

20. On the forum Darkode.com, a forum known to your Affiant to be devoted to the exchange of criminal services and tactics, the user Severa provides the ICQ number 104967, the email address peter@severa.biz, and the jabber address jabber@honese.com. These same contact details are also provided at the forums verified.cm, zae-biz.com, directconnection.ws, and pustota.tw. All of these forums are known to your Affiant to be utilized by online criminals for the exchange of criminal services and tactics. In addition, there are accounts in the name of Severa at many other forums which utilize a variation of the above contact details. For example, the user Severa is also often linked to the email address info@emailpromo.org. Examination of the registration details for the domain severa.biz, as observed in the email address peter@severa.biz, reveal that the registrant email is info@emailpromo.org. That would indicate that Severa is also utilizing the email address info@emailpromo.org.

21. On 11/27/2011, the user Severa posted a message on the criminal forum Darkode which stated "My name is Peter Severa, I am one of the oldest Russian spammers. I offer webmail mailing service with good inbox rate on many Russian forums for 10 years".





Infections

22. Alaska has been affected by Kelihos malware. Victims infected by Kelihos fall into two categories: (1) those communicating via a private IP address, such as those whose computer is connected to the internet via Wifi or gateway router; and (2) those utilizing a public IP address, such as those connected via an Ethernet cable directly to their cable modem. A private IP address cannot be directly accessed by the Kelihos botnet. However, a public IP can be directly accessed by, or communicated with, the Kelihos botnet. Accordingly, communications to a private IP address are first sent to its associated router, which is publicly accessible. The Kelihos botnet uses those computers with publicly accessible IPs to form the backbone of its P2P architecture.

23. There are several methods known to your Affiant to determine those computers worldwide which are infected with Kelihos malware and which IPs are publicly accessible. One method is to resolve the "Golden Parachute" domains. Golden Parachute is a name utilized by Kelihos actors to describe those web servers utilized for functions including hosting and the distribution of malware executables. Examples of the Golden Parachute domains include gorodkoff.com and bayermun.biz. These domains utilize a Domain Name System (DNS) resolution technique known as "Fast Flux". DNS is a system that maps IP addresses to easier to understand letters and numbers. For example, it is easier for most people to remember the domain name "google.com" than it is to remember the IP address 216.58.194.46. Fast Flux is a technique designed to defeat detection measures by rapidly changing the IP address of an associated domain. Whereas a traditional website might cache its DNS records for minutes or hours at a time, Fast Flux domains have a very short cache value. In the case of Kelihos, the cache value is set at "0". This practical effect of a "0" TTL field is that essentially every time a



domain resolution query is issued for a Golden Parachute domain, the associated IP address rotates through a list of hundreds of possible IP addresses. In the case of Kelihos, victims with public IP addresses are utilized as proxies to the true backend domain IPs, so resolving Kelihos Golden Parachute domains such as with the query “dig +short gorodkoff.com” would result in an IP address belonging to a Kelihos victim. Therefore, by resolving these domains many times, it is possible to create a list of Kelihos victims.

24. Another method used for determining victims of Kelihos is known as “crawling”. Crawling is a technique to enumerate the locations and features of applications and devices on the Internet. Applied to malware, crawling is a technique in which the researchers communicate in a successive manner to subsequent infections, often by communicating with the botnet as if they too are infected. With a P2P botnet, over time this can result in the discovery of many of the infected peers. Kelihos victims distribute a list of up to 500 similarly infected “peers”. This list is dynamic, meaning that the contents are frequently updated and the list itself is frequently exchanged with other Kelihos infections as a method of maintaining connectivity. Therefore, “crawling” over a sufficient length of time, such as weeks and months, can result in a good sense of the overall number of infected systems, as well as the timeframes for when systems become infected, and when they cease to be infected.

25. Utilizing these techniques, your Affiant was able to identify several apparent victims of Kelihos malware in Alaska. For example, two victims’ public IP addresses were actively communicating with the Kelihos botnet in September and October 2015, respectively. The victims stated that they did not authorize the installation of any malware on their computers, to include Kelihos. In both cases, your Affiant was unable to actually locate evidence of the Kelihos malware on the computers. Because the computers had ceased communicating with the



Kelihos network by the time your Affiant was able to examine the computers, your Affiant believes that the infections had already been discovered and removed by antivirus products.

26. Your Affiant has further identified victims of Kelihos in Alaska that were previously more difficult to detect due to the utilization of private IP addresses. Private IP addresses are those IP addresses belonging to specifically designated class designations of either A, B, C. Private IP addresses are frequently utilized in an effort to reduce the overall number of allocated IPv4 IP addresses, and to better facilitate the construction and maintenance of private networks. IPv4, or Internet Protocol version Four, is the most commonly encountered IP address format in the United States, and the format upon which most US households depend. For example, in most households, all computers, tablets, and telephones connected to the Internet via a WiFi router, will be assigned private IP addresses. In that scenario, it is only the WiFi router itself that has a publicly accessible IP address. For devices outside this private network to communicate with one of the devices on the private network there must be address translation according to a table maintained by the router itself. In this process, the IP addresses of devices other than the router remain unknown to devices external to the private network. This is in contrast to a computer which itself has a publicly accessible IP address. Then, communications are sent directly to and from the computer in a greatly simplified manner. For this reason, Kelihos and similar botnets place special emphasis on those infections that are publicly accessible, for the simple reason that they can easily communicate with other infected systems, and with the backend servers administrating the botnet.

27. One such Alaskan based IP address, utilizing a private IP address, was observed communicating with the Kelihos botnet in March, 2016. Subsequent analysis of the computer by your Affiant revealed a number of factors correlated with a Kelihos infection. There were many



entries in the victim's Run Registry Entry, to include an entry utilizing the typical Kelihos naming convention. This entry pointed to an executable file one megabyte in size, again, consistent with Kelihos malware. The file itself was examined independently by industry experts who specialize in the study of Kelihos and other botnets. The expert's determination was that the malware was Kelihos, and that the encoded affiliate ID was qthotfd. Your Affiant conducted an analysis by uploading the executable file to virustotal.com, an antivirus composite tool. The majority of the antivirus products on virustotal.com identified the executable file as a form of malware. Your Affiant conducted further analysis of the changes made to Windows registry files when the executable was run. Those changes were consistent with the behavior of Kelihos malware, to include creating an entry in the "Run" registry key titled "CrashReportChecker" that was linked to the malicious file itself.

#### Job Requests

28. Another method used by your Affiant to evaluate the damage caused by Kelihos malware is to examine the distributed email messages. Kelihos has resulted in hundreds of thousands of unwitting third parties receiving unsolicited email messages directing them to purchase illicit pharmaceuticals, penny stocks, or participate in mule/escrow operations. These messages are first distributed to those infected with Kelihos malware in the form of "job requests". These job requests are text files containing a large number of descriptive fields and data which serve as instructions to those computers infected with Kelihos malware.

29. For example, in a job request dated 12/17/2015, one of the fields contained a list of domains including gorodkoff.com, mydear.name, and goloduha.info. Your Affiant knows these domains to be "Golden Parachute" domains, utilized by Kelihos operators for the distribution of the Kelihos binary. It is possible to download the Kelihos malware directly from



the aforementioned Golden Parachute domains, and from some victims infected with Kelihos malware. If a Kelihos affiliate name is known, it is possible to download the malware by issuing commands such as "wget gorodkoff.com/affiliate.exe." In this manner your Affiant has downloaded samples of Kelihos malware. Your Affiant has conducted further analysis of the sample's behavior, such as how it modifies the underlying computer system, and how it tests network connectivity. Your Affiant has also consulted with internet security experts and utilized Internet based malware identification tools in order to confirm that the samples in question are Kelihos.

30. Another field within a Kelihos job request contained 3333 separate email addresses. The job request directed Kelihos infections to distribute emails containing the message: "Be girl's idol. Extended vigor in bed <http://indirect.ycuqobot.ru>". This included URL led to a webpage labeled the "Canadian Health and Care Mall" which offers for sale Viagra and Cialis, including generic versions, in addition to other common pharmaceuticals such as Levitra and Propecia.

31. Another email message contained within the same job request, directed to a separate list of 3333 email addresses, featured email addresses principally assigned by United States educational and government email addresses. Some of those email addresses included Alaskan government issued addresses for personnel in Anchorage and Kenai school districts. The email directed recipients to contact Gronghold Trade LP for job opportunities in which the recipients perform marketing and escrow sales services. The email stated that the average escrow amount was \$84,457. Your Affiant recognizes this email as a common work from home scheme, whereby the recipients receive funds either stolen or laundered and are directed to transmit the funds to a further recipient, in exchange for a flat fee or a percentage payment. Your



Affiant knows that victims, or mules who engage in such conduct can be held liable for the entire amount that traversed their accounts and are generally unaware of the criminal intentions of those who send such solicitations.

Affiliate Payment Model

32. Kelihos uses an affiliate payment model for distribution. Affiliate models are common on the Internet, to include in criminal schemes. An affiliate model allows a website or service operator to pay independent contractors, or affiliates, for generating traffic or subscriptions. For example, affiliate models are common on pornography sites whereby a referrer would be paid a certain amount for every new subscription he generated. The referrer would have wide latitude in how he generated the subscriptions.

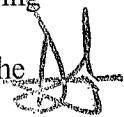
33. In this same model, Kelihos administrators pay affiliates based upon every infection that they generate. Your Affiant has downloaded a portion of the "Smoney" Kelihos portal. Smoney is the name Kelihos actors gave to a backend database devoted to the administration of their affiliate system. One portion of this system is an HTML page titled "loads01\_rules.html". This page, when translated from the Russian, states:

"Attention! This system is designed exclusively for Windows-based testing for vulnerabilities. Administration is not responsible for the use of this system for any purpose.

The current system ip: 89.144.2.118 176.103.48.27

Statistics and exe files are accessible via any of those IPs, they both lead to the same place, and it doesn't matter which one you use. Pick any as your main one, and save the others as backups in order to always be able to download the fresh exe or get access to the statistics.

This system is refreshed every 10 minutes. Additionally, there is a delay in the ping-backs of the exe of approximately 10-15 minutes. Attention: there is no need to reload the




statistics or the files very frequently. You may be blocked if you send more than 10 requests to my server within 10 minutes.

You may load it in parallel with anything you want. This is your right, and I do not insist on exclusivity. But I evaluate each affiliate's average bot lifespan, and since I'm paying for loads of a Socks bot, I need that Socks to work. It's prohibited to load winlockers and fake AV, in short anything that will block running processes and prevent me from using the bot. You can load anything else."

34. The page then provides the pricing paid to affiliates per infection. Infections in the United States are paid at \$.60 per infection, while infections in Australia, Canada, and the United Kingdom are paid at \$.40. Infections of some countries pay affiliates only \$.02. Affiliates are not paid for Russian infections. The rules page goes on to state:

"Payouts for the loads are made upon request to Bitcoin or WebMoney no more frequently than once per day. There is no delay. Everyone who has begun working with the system has automatically agreed to these conditions. Payment may be refused to anyone who has violated these conditions.

It is prohibited to remove my exe from memory, delete/alter my file, registry keys, or any data saved on the client. Accounts caught doing any of these will be blocked without pay."

35. Based upon my training and experience, your Affiant knows that this page is describing a complex scheme in which the affiliates receive relatively high payment for infecting computers in Western nations with the Kelihos malware, and that affiliates are allowed to load other types of malware in conjunction with Kelihos, so long as the malware doesn't interfere with Kelihos functionality, to include SOCKS, a form of proxy communication necessary for the P2P communication to function. This description is similar to observations by your Affiant 



whereby Kelihos is often bundled with other forms of malware, and utilizes many different methods of initially infecting victims.

36. The mention of “registry keys” in the final paragraph is consistent with your Affiant’s analysis of Kelihos malware, that is that the malware avoids many Antivirus products as well as the user’s own attempts at removal by creating an entry in the Windows Registry File allowing the malware to run on startup. This means if the victim stops the currently running Kelihos process, the malware will still run again the next time the computer is rebooted.

#### Servers

37. Your Affiant has identified two servers, associated with the Kelihos botnet, that are located in Luxembourg. In coordination with Luxembourg authorities, your Affiant receives data from these servers, equivalent to data that would be gathered in the United States using a wiretap. Examination of this data has revealed multiple associations between the Kelihos malware, its backend architecture, Severa, and his presumed true identity of Petr Levashov of Saint Petersburg, Russia.

38. One of the servers, bearing the IP address 94.242.250.88, in addition to functioning as a portion of the Kelihos backend, appears to be used by Levashov as a proxy, meaning that some portion of his Internet activities are directed through the server. As a result, your Affiant has been able to observe backend panels, or websites, that provide status updates on the botnets. Such panels are very commonly encountered in the investigation of botnets as they make administration and troubleshooting much easier for the operators. The Kelihos panel is constructed as a website and includes information such as the status of various servers, and the status of the Golden Parachute Domains. Gorodkoff.com, goloduha.info, and others, are specifically referenced, with color codes used to indicate their readiness status. Another portion



of the webpage depicts various backend servers, the spam messages they are being used to distribute, and data such as the speed at which the messages are being distributed. An example appears below.

**Ip: 193.28.179.38**

Sat, 20 Feb 16 18:25:29 +0400

List: ../lists/pharma\_b+pharma+trade

Body: Perfect method to ha ...

ldrugmarket.ru/

Subject: Do you wan ... his night?

Counter: 712910562 (1424874532)

Speed: 79677 m/h

**Ip: 176.103.48.27**

Sat, 20 Feb 16 18:47:54 +0400

List: pharma\_b+pharma+trade

Body: Giveto your babe nig ...

ng.hxilgusk.ru/

Subject: Evoke your ... admiration

Counter: 608715981 (1424874532)

Speed: 10323 m/h

39. Other portions of this panel include antivirus and blacklisting reports. This indicates that the operators actively monitor whether or not their various servers have been identified by antivirus or other blacklisting services, as such blacklisting could reduce the reliability access of their network. Of note, the panel indicates that both of the servers hosted in Luxembourg appear to be tracked by at least one antivirus vendor, as their IP addresses appear within a list of other IPs all believed to be associated with Kelihos, and is correspondingly linked to an antivirus product.

40. In addition to the backend, the server appeared to contain copies of many of the distributed spam email messages. Subject lines of emails that appear to have been sent to gci.net email accounts include "Very good way to reveal your intimate life," "No amorous failure risk," "Attack your woman harder," and "Are you ready to please your female partner tonight?" These emails contained links to websites that appear to facilitate the purchase of gray market pharmaceuticals.

41. Also appearing to have been sent to gci.net email accounts were emails with the subject lines "This Company looks ready for a major run this week!," "Big Gainers Since My

Alert!,” “It is about to wake up and ROAR!,” and “Its trading levels could change in no time (MUST READ)”. The content of all of these emails was similar as they are intended to persuade the recipient to purchase a specific U.S. listed stock. One example of the email content:

This Stock is our New WILD Sub-Penny Pick! Get Ready for Multi-Bagger Gains!

Top 10 Reasons Why We Love This Pick!

Company Name: APT SYSTEMS INC

Traded as: A\_PT-Y

Long Term Target: \$1.70

Trade Date: February, 29th

Closed at: 0.30

42. Your Affiant is familiar with these types of stock manipulation schemes, known as “pump and dump.” These schemes, which usually manipulate low priced, or “penny” stocks, attempt to change stocks by drastically increasing volume. For stocks in which there are few overall shareholders, or which are generally not traded in large quantity, a small increase in purchase activity can result in a large increase in stock price. Your Affiant has examined historical prices for several stocks for which Kelihos has conducted spam email campaigns and noted that such campaigns usually result in a temporary increase of the stock price of anywhere from 30-80%.

#### Email and iCloud Accounts

43. As previously described, your Affiant has conducted open source research into the Kelihos malware and its purported operator, Severa, noting the historical usage of the ICQ number 104967, and the use of jabber accounts such as jabber@honese.com, and the email account peter@severa.biz. The use of these communication accounts goes back many years, and



in fact, appear to have been utilized by Severa since 2002. Your Affiant searched for these, and other communication accounts, in the data relating to communications on the two Luxembourg based servers. There are tens of thousands of references to the ICQ number 104967, most contained within status messages that state "Yep, I'm here. Severa7104967."

44. There were many email messages sent to the email account peter@severa.biz. For example, one sent on March 2, 2016 from investmentsoffshore@gmail.com to peter severa <peter@severa.biz> contains the subject line "Fwd: Need mailing". The content of the email is:

Hi Peter,

I need mailing, Ecuador, Colombia and Bolivia.

How much?

Do you receive Paypal?

Regards, Robert

45. The reply, sent from peter@severa.biz to investmentsoffshore@gmail.com on March 2, 2016 states:

Hi, i accept webmoney or bitcoin.

Yes, i have these countries, mailing costs 500 usd per 1 mil emails, 750 usd per 2 mil, 1k per 3 mil.

Best regards,

Peter Severa

E-mail: peter@severa.biz

46. Another email account frequently observed within the Luxembourg server data is pete777@mail.ru. There were thousands of what appear to be automated logins to the mail.ru website tied to this email account.

A handwritten signature in black ink, appearing to be 'AS' or similar, with a stylized flourish at the end.

47. Apple documents indicate that the email address [pete777@mail.ru](mailto:pete777@mail.ru) is associated with an Apple iCloud account in the name of Petr Levashov of the Russian Federation. The Apple DS ID number is 1972828024. The Account Type listed is Full iCloud, with a creation date of September 2, 2012. The Account Status is listed as Active. A second email address is also associated with this iCloud account, [levashov@knyazev-spb.ru](mailto:levashov@knyazev-spb.ru). Further subscriber information indicates that this account was registered using the IP address 83.243.67.25.

48. This is the same IP address utilized to register a Google account, [peteknyazev777@gmail.com](mailto:peteknyazev777@gmail.com). The accounts [peteknyazev777@gmail.com](mailto:peteknyazev777@gmail.com) and Apple DSID 10090662027 share extensive overlap of IP addresses utilized to access these accounts, to include 91.122.62.16. Additionally, access logs indicate that these accounts share temporal overlap with IP addresses as well, meaning that the same IP addresses are utilized during similar time periods. Based upon my training and experience, your Affiant knows this to be characteristic of the same individual accessing the same accounts.

49. "Foursquare" is a social media application that provides recommendations on restaurants and shopping establishments to users. A Foursquare account in the name Petr Levashov, registered with email address [pete777@mail.ru](mailto:pete777@mail.ru), also displays the same pattern of temporal overlap within the IP access logs, when compared to the previously mentioned Apple and Google accounts.

50. One IP address appearing within Levashov's Foursquare account is 85.17.31.90. This IP address also appears within Levashov's Apple DS ID iCloud account 1972828024, and the Google account [pr@hottaby4.ru](mailto:pr@hottaby4.ru). Google records indicate that [pr@hottaby4.ru](mailto:pr@hottaby4.ru) has been accessed by only two other IPs, one of which, 94.242.250.88, is the IP address of the Luxembourg based server analyzed by your Affiant.



51. The server data also contains many references to Petr Levashov. For example, an email sent on February 26, 2016 from no\_reply@email.apple.com to petr@hottaby4.ru with the subject line "Your app(iOS) status is In Review" is addressed to Petr Levashov and contains a status update on an iOS application. There are many such emails sent from this Apple email account to petr@hottaby4.ru.

52. Apple documents indicate that the email address petr@hottaby4.ru is associated with an Apple iCloud account in the name of Petr Levashov of the Russian Federation. The Apple DS ID number is 10090662027. The Account Type listed is AppleID, with no creation date listed. The Account Status is listed as Active. Further subscriber information indicates that the start date for Apple services was December 15, 2015. This account was accessed in December 2015, February 2016, and March 2016 utilizing an IP address known to be associated with the Kelihos back end server. Two of the Apple services used by this account are iPhone Dev Center and Xcode. The use of these services is consistent with the coding and development of Apple iOS applications.

53. Based upon my training and experience, your Affiant believes that this pattern of temporal overlap of IP addresses is indicative that the accounts pete777@mail.ru, peteknyazev777@gmail.com, pr@hottaby4.ru, peter@severa.biz, petr@hottaby4.ru and the associated Apple iCloud accounts in the name of Petr Levashov are all consistently accessed by the same individual.

#### **BACKGROUND CONCERNING APPLE ID AND ICLOUD**

54. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.



55. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user’s Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain





enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

56. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

57. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to

access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

58. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

59. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.



60. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

61. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps

may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

62. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

63. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

64. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and



because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crimes under investigation.

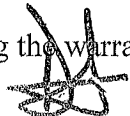
65. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

66. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

67. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

68. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant



to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Attachment A. Upon receipt of the information described in Attachment A, agents will review that information to locate the items described in Attachment B.

69. This search warrant authorizes the Government to retain after its review all of the items described in Attachment A. This authorization is justified in this case, in part, because:

- a. The investigation is not yet complete and accordingly, it is not possible to predict all possible defendants against whom evidence from the email account and associated records might be used. That evidence might be used against persons who have no possessory interest in the account's communications and associated records, or against persons yet unknown. Those defendants might be entitled to a copy of communications and associated records in discovery that are not within the scope of Attachment B. Retention of all of the account's communications and associated information assures that it will be available to all parties, including those known now and those later identified;
- b. The Government's possession of these materials will not deprive Apple or the owner of the account from possessing the same items;
- c. Should the execution of the warrant uncover data that may later need to be introduced into evidence during a trial or other proceeding, the authenticity and the integrity of the evidence and the government's forensic methodology may be contested issues. Retaining all of the items produced by Apple can help the Court resolve such claims;



- d. Apple will likely not close the account in response to the search warrant.

Accordingly, ongoing access and use of the account by the account's user(s) may alter or eliminate the items. Thus, retaining the items produced by Apple assures preservation of these records; and

- e. The act of destroying items produced by Apple could create an opportunity for a defendant to claim that the destroyed items contained evidence favorable to him. Maintaining a copy of the items would permit the Court and government, through an additional warrant if necessary, to investigate such a claim.

### **CONCLUSION**

70. Based on my training and experience, and the facts as set forth in this affidavit, I believe there is probable cause that on computer systems in the control of Apple, as set forth in Attachment A, there exists evidence and instrumentalities of violations of Title 18, United States Code, Section 1030 as set forth in Attachment B.

71. Based on the foregoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Apple who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

**FURTHER YOUR AFFIANT SAYETH NAUGHT.**

^

Signed: \_\_\_\_\_

Signature Redacted

Elliott Peterson, Special Agent

Date: \_\_\_\_\_

5/20/2016





Subscribed and sworn to before me this 20 day of May, 2016.

/s/ DEBORAH M. SMITH  
CHIEF U.S. MAGISTRATE JUDGE  
SIGNATURE REDACTED



---

DEBORAH M. SMITH  
U.S. MAGISTRATE JUDGE



MAY 20 2016

**ATTACHMENT A**

**Information to Be Disclosed by Apple Inc. (the "Provider") and**


**Searched by the Government**

This warrant applies to information associated with an Apple iCloud account that is associated with DS ID number 1972828024 from September 2, 2012 to present that is stored at premises controlled by Apple Inc., a company that accepts service of legal process at subpoenas@apple.com, 1 Infinite Loop, Cupertino, CA, as set forth below.

For the time period from September 2, 2012 to present, to the extent that the information is within the possession, custody, or control of the Provider, including any pictures, videos, emails, records, files, logs, GPS-related information, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the account listed above:

a. The contents of all files and records associated with the account, including stored or preserved copies of files and records (including emails, pictures, videos, etc.), draft files and records, the source and destination addresses associated with each file and record, the date and time at which each file and record was stored and/or accessed, and the size and length of each file and record;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address



MAY 20 2016

used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, videos, documents, notes, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

A handwritten signature in black ink, consisting of stylized, overlapping loops and lines.

**ATTACHMENT B**

**Particular Things to be Seized**

All information described above in Attachment A that constitutes evidence or instrumentalities of violations of Title 18, United States Code, Section 1030 (Computer Fraud) from September 2, 2012 to present, including:

- (a) Communications sent and received, draft emails, deleted emails, contacts, solicitations, efforts to find potential customers or affiliates, price negotiations, transaction records, payment information, bank account information, contact information for persons or businesses solicited, inquiries, pictures, videos, emails, address books, contact or buddy lists, calendar data, GPS-related information, financial records, music, movies, bookmarks, notes, reminders, and other correspondence and records related to the creation or distribution of malware, botnets, or spam email; and
- (b) Records relating to who created, accessed, or used the Apple iCloud account that is associated with Apple DS ID number 1972828024 or to modify any aspect thereof, and his/her whereabouts, including the subscriber's name, the subscriber's physical address, the subscriber's telephone numbers and other identifiers, the subscriber's alternative e-mail addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, the log-in IP addresses associated with session times and dates, the methods of connecting, the log files, and the means and source of payment.



With respect to information disclosed to the government pursuant to Attachment A, which falls outside the scope of the categories described above in Attachment B, the government may retain such information until one year after the investigation, and any trial(s) or appeal(s) that may arise from the investigation have been concluded, or upon conclusion of any collateral attack or post-conviction relief, whichever is later, but will return or destroy such information at such time unless prior court approval is obtained. The government must apply for an additional search warrant if it seeks to search for information outside the scope of the categories described in Attachment B.

A handwritten signature in black ink, appearing to be a stylized 'J' or 'L' with a horizontal line extending to the right.

MAY 20 2016